## REMARKS

In accordance with the foregoing, claims 1-7, 13, 16, and 19-22 are amended and new claim 23 is presented. No new matter is presented, and accordingly approval and entry of the amended claims and new claim are respectfully requested.

Claims 1-23 are pending and under consideration. Reconsideration is requested.

**Claim Amendments**

Independent claim 1 is amended herein to recite a position information management system that "can decrypt the previously recorded encrypted position information only after the terminal sends a key used to decrypt the previously recorded encrypted position information to the position recording apparatus and the position recording apparatus receives the key from the terminal." Independent claims 16, 17, and 22 are similarly amended. Dependent claims 2-7, 13, 16, and 19-21 are amended accordingly.

Support for the amendments is found, for example, on page 13, lines 21-24 of the specification. No new matter is being presented, and approval of the amended claims is respectfully requested.

**Traverse of Rejections**

**I.** In item 4 of the Office Action, the Examiner rejects independent claims 1, 16-17, and 22 (and dependant claims 2, 5, and 18-20) under 35 U.S.C. §102(e) as being anticipated by Giniger et al. (U.S.P. 6199045). (Action at pages 4-9). The rejections are traversed.

As set forth MPEP §706.02 entitled Rejection on Prior Art, anticipation requires that the reference must teach every aspect of a claimed invention. Applicants submits that Giniger does not support an anticipatory-type rejection by not describing features recited in each of the independent claims. For example, independent claim 1 recites a system including:

a) " a terminal measuring the position of the mobile body, encrypting measured position information by predetermined encryption means and transmitting the encrypted position information (emphasis added);" and

b) "a position recording apparatus, remotely located from the terminal, communicating with the terminal through a radio network, receiving the encrypted position information transmitted from the terminal through the radio network and recording the encrypted position information in an encrypted state (emphasis added)," and

c) "wherein the position recording apparatus can decrypt the previously recorded encrypted position information only after the terminal sends a key used to decrypt the previously

recorded encrypted position information to the position recording apparatus and the position recording apparatus receives the key from the terminal (emphasis added)." Independent claims 16, 17, and 22 have similar recitations.

That is, according to an embodiment of the present invention, the encrypted positional information of the mobile body is transmitted to, and recorded on the position recording apparatus before a key used for decryption of the recorded positional information is transmitted to the position recording apparatus. By contrast, Giniger teaches:

> Next, the central site server 107' transmits, via the established circuit-switched data connection, a request to the mobile unit 103' to initiate receipt and processing of position information (step 615). . . In response to receipt of the central site server's message, . . . After its position has been determined, the mobile unit 103' transmits this information to the central site server 107' via the established circuit-switched data connection (step 618). . . .The central site server 107' receives the position information from the mobile unit 103' and stores this in a second data record associated with the mobile unit 103' (step 619). . . ., the retrieved information is then transmitted to the mobile unit 103' via the established circuit-switched data connection (step 621).

(Emphasis added, See, for example, Fig. 6A, and col. 18, line 34 - col. 19, line 8).

That is, as clearly illustrated in Fig. 6A, Giniger does not teach transmitting positional information until after it is acknowledged that a secure connection is established, and does not teach a system including " position recording apparatus can decrypt the previously recorded encrypted position information only after the terminal sends a key used to decrypt the previously recorded encrypted position information, as recited by claim 1, for example.

In item 2 of the Office Action, entitled "Response to Arguments" the Examiner asserts:

> Giniger discloses that the mobile unit transmits to the central server a message that includes a challenge field encrypted using the public key of the central server and the mobile unit's public key certificate (see col. 17, lines 29-57). Thus, as disclosed in the previous response, the mobile unit's transmits decrypting data to the central site server. Also, before the symmetric key was sent to the central server, the central server received from the mobile unit the public key certificate, and the central server cannot decrypt data it does not have. The mobile unit has to first encrypted the information using the symmetric key, and when received by the central server, the central server has to inherently recognized that the data has been encrypted using the symmetric key. Therefore, by receiving encrypted information form the mobile unit, the central server receives decryption data from the mobile unit.

(Action at pages 2-3).

However, Applicants respectfully point out that by contrast, Giniger merely teaches:

> [I]f a secure connection is desired by the user or required by the central site server 107', then the process continues at step 604, where the central site server 107' uses the established circuit-switched data connection to send its public key

> certificate to a security unit contained within the mobile unit 103'. In step 605, the mobile unit 103' uses the established circuit-switched data connection to transmit back to the central site server 107' a message that includes a challenge field encrypted using the public key of the central site server 107' and the mobile unit's public key certificate. Next, at step 606, the central site server 107' decrypts the challenge field that was received from the mobile unit 103' in step 605, and sends both the challenge field and a symmetric key back to the mobile unit 103' via the established circuit-switched data connection. This message is transmitted in an encrypted form using a public key envelope. Upon receipt of the message, the security element in the mobile unit 103' decrypts the public key envelope and stores the symmetric key for use in all future transmissions with the central site server 107' for the duration of the call (step 607). That is, all subsequent transmissions with the mobile unit 103' will be encrypted using the symmetric key.

(Emphasis added, see, for example, col. 17, lines 27-53).

That is, Giniger teaches not sending positional information *arguendo* step 618 until after:

1) the central site server sends a public key certificate to the mobile unit;

2) the mobile unit sends a challenge field to the central site server;

3) the central site server decrypts the challenge field that was received from the mobile unit;

4) the central site server sends a challenge field and a symmetric key to the mobile unit in an encrypted form using a key; and

5) the mobile unit decrypts the public key envelope and stores the symmetric key for use in future transmissions with the central site server for the duration of the call.

While Applicants appreciate that broadly written claims are broadly interpreted, Applicants respectfully submit that one of ordinary skill in the art would not interpret the exchange of challenges discussed by Giniger in example steps 601 - 609 as transmitting encrypted positional information for the mobile unit to the server. Further, Giniger does not teach sending a key after the positional information is transmitted, as recited by claim 1 for example.

Since features recited by independent claims 1, 16-17, and 22 (and dependant claims 2, 5, and 18-20) are not disclosed by Giniger, the rejection should withdrawn and claims 1-5, 16-20, and 22 allowed.

**II.** In items 6-9 of the Office Action, the Examiner rejects dependent claims 3-4, 6-15, and 21 under 35 U.S.C. §103(a) as being unpatentable over Giniger in view of combinations of Olsson (U.S. Pub. No. US 2002/0080968), Pirila (U.S.P. 6674860), and Walsh et al., Pub. No. US 2004/0033795. (Action at pages 9-20). The rejections are traversed.

Claims 3-4 and 6-15 depend from independent claim 1, which, for reasons argued above, patentably distinguish over Giniger and should be allowed. Claim 21 depends from

parent claim 17, which, for reasons argued above should be allowed.

Applicants submit that nothing in the teachings of Olsson, Pirila, nor Walsh fail to cure the deficiencies argued above, and thus it is respectfully submitted that dependent claims 3-4 and 6-15 patentably distinguish over the prior art.

**Summary**

Since features recited by independent claims 1, 16-17, and 22 (and respective dependent claims) are not taught by an *arguendo* combination of the art relied on by the Examiner, the rejections should be withdrawn and claims 1-22 allowed.

**New Claim**

New claim 23 recites features in a different manner and recites a method including "transmitting an encrypted position of the mobile body from to an apparatus that is separate from the mobile body; storing the encrypted position of the mobile body in an encrypted state in the apparatus; transmitting a key used for decrypting the encrypted position from the mobile body to the apparatus."

Support for claim 23 is found, for example, on page 13, lines 21-24 of the specification. No new matter is being presented, and approval and entry are requested

**Conclusion**

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: April 24, 2008

By: Paul W. Bobowiec

Paul W. Bobowiec
Registration No. 47,431

1201 New York Avenue, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501